NATIONAL LAW ENFORCEMENT AND CORRECTIONS TECHNOLOGY CENTER
A program of the National Institute of Justice

From Spring 2007 *TechBeat*

TECH b•e•a•t

Dedicated to Reporting Developments in Technology for Law Enforcement, Corrections, and Forensic Sciences

Biometric Basics

Biometrics is a general term used alternatively to describe a "characteristic" or to describe a "process." As a characteristic, biometrics refers to anatomical, physiological, or behavioral characteristics that can be used for automated recognition. Signatures and the sound of the voice fall into the behavioral category. Blood type and DNA are physiological characteristics. Anatomical characteristics—such as fingerprints, the iris, hand geometry, and the face—are the most frequently used biometrics because they can be measured quickly and easily at a reasonable cost.

As a process, biometrics refers to automated methods of recognizing an individual based on measurable anatomical, physiological, or behavioral characteristics. Biometric (process) systems typically have five components:

- A sensor for capturing and digitizing data from enrollees.
- Processing algorithms for forming biometric templates.
- A unit for storing data and templates.
- Matching algorithms for comparing new templates with the stored templates.
- A decision process for accepting or rejecting individuals.

Three main kinds of errors are used to rank the performance of biometric systems:

- The failure-to-acquire rate is the percentage of times a system fails to capture a useful biometric from an individual.
- The false-accept rate is the percentage of times an individual is incorrectly matched to the template of another individual.
- The false-reject rate is the percentage of times an individual is not matched to the individual's existing template.

Biometric technologies have indisputable advantages for establishing and verifying identity: No one can forget biometric characteristics, lose them, or give them to someone else. Additionally, they are either unchangeable or highly resistant to being changed. In recent years, biometric technologies have become better, faster, easier to use, and cheaper. The number of law enforcement and corrections biometric applications is growing rapidly. Potential users should learn as much as possible about the technology and systems to ensure they produce good results.

Five Leading Biometric Technologies

Fingerprint readers capture an image of a fingerprint, extract a pattern, and mathematically encode the pattern into a template representing the image. Optical devices capture samples using light and are the only ones designed with enough sensor area to capture the fully rolled fingerprints needed for FBI identity checks; processing all 10 fingers makes operating speed slow. Capacitive devices, usually designed to require one fingerprint, detect the electrical field where a finger touches the sensor; these readers are fast, compact in size, less expensive, and typically used for access control. Fingerprint readers are the most popular biometric devices (nearly 80 percent of the world market), and huge databases of print images are available. False-accept rates are less than 1 in a million; false-reject rates may be more than 2 percent.

Optical devices use several methods, but basing identification on minutiae points (where print ridges begin, terminate, or split) is the most popular. A fingerprint typically has 30 to 40 minutiae. (The FBI finds that no two individuals have more than eight minutiae points in common.)

Iris recognition technology captures the image of the iris using a high-quality digital camera. Its complex pattern is converted using algorithms into a 512-byte template called an IrisCode(r), invented and patented by Dr. John Daugman in 1994. Scanning can be done from a few inches to a yard away and takes just seconds; the small template allows a database to be searched rapidly. Tests show that iris scanning has a false-accept rate of 0.1 percent, with a false-reject rate of 1 to 2 percent.

A disadvantage of the technology is that no huge database exists (such as the FBI's for fingerprints). In addition, one cannot leave an iris "print" at the scene of a crime and failures to acquire a good iris image may be as high as 10 to 15 percent in bright outdoor lighting, although training usually lowers that percentage.

The iris structure is set by age 1 and appears to remain the same throughout life. The iris is like a human barcode: No two are the same.

Face recognition technology captures the image of a face with a camera and constructs a template. Early face recognition algorithms used simple geometric models, but the recognition process has matured into a science of sophisticated mathematical representations and matching processes. Major advances in the past 10 to 15 years have made the use of face recognition more common. The technology is now used both to verify a claimed identity and to identify someone by searching a database for possible matches. A clear advantage of face recognition technology is that images can be captured without physical contact; devices could become valuable surveillance tools. Continuing technical challenges are that systems often cope poorly with changes in lighting or with images taken from the side or above. A shift from low-resolution two-dimensional images to high-resolution two- and three-dimensional images shows potential for improving system accuracy.

The results of recent Face Recognition Vendor Tests (http://face.nist.gov/frvt) show that the performance results for face recognition technology are similar to those for iris recognition technology, with a false-accept rate of 0.1 percent and a false-reject rate of 2 percent.

Hand geometry scanners use a CCD (charge-coupled device) camera to capture the dimensions of a hand placed on a plate palm down, guided by five pegs that sense when the hand is in position. Mirrors allow data to be gathered from the side and top of the hand. A scanner takes 90 measurements—such as lengths and widths of the fingers, distances between knuckles, and surface areas—and constructs a template. Enrollment usually requires capturing three images. Verifying that a person is who he or she claims to be involves swiping an identity card or entering a personal identification number right before scanning a subject's hand for comparison against the stored template; the system generates a similarity score and accepts or rejects the subject. Commercially available since 1986, these devices capture measurements in about 1 second. They are noninvasive, easy to use, reasonably accurate, and highly acceptable to the public. Unlike fingerprint readers, hand geometry scanners are not affected by lines, scars, dirt, and other surface details. This technology serves well for fast, easy, and frequent identity checks-for example, to track the crossings of frequent travelers at borders, to track attendance at workplaces, and to control access in general.

Over time, the shape of the hand does not change significantly, but hand geometry is not unique. Too many hands are similar in size and shape for this biometric to deliver high-security verifications.

Dynamic signature identification systems use software to measure the speed, direction, and pressure of pen strokes while signing an electronic tablet. Enrollment usually requires a set of sample signatures. From the data collected for each feature, the software constructs a digital template for comparison with future signatures. Although a forger can replicate a signature with practice, it is nearly impossible to duplicate how a person writes his or her signature, which makes the dynamic method a reliable biometric. Many patented technologies for signature identification are available, and systems are inexpensive. This biometric, though, is prone to high false-reject rates because signatures may vary from one signing to another. The development of techniques for differentiating the parts of a signature that are consistently the same from those that vary with each signing has reduced error rates.

Because signatures are required in everyday transactions, this biometric has a great advantage: public acceptance.

Editor's note: DNA matching is a method of recognizing a person based on chemical sequences at specific places along the DNA molecule. This tool for establishing identity and proving guilt or innocence, however, cannot be regarded as a biometric because much of the process is not yet automated.

For more information about biometrics, visit "Introduction to Biometrics" (under "Additional Resources") and other webpages at www.biometricscatalog.org/default.aspx, or contact William Ford at the Office of Justice Programs' National Institute of Justice, William.Ford@usdoj.gov.

This article was reprinted from the Spring 2007 edition of *TechBeat,* the award-winning quarterly newsmagazine of the National Law Enforcement and Corrections Technology Center system, a program of the National Institute of Justice under Cooperative Agreement #96–MU–MU–K011, awarded by the U.S. Department of Justice.

Analyses of test results do not represent product approval or endorsement by the National Institute of Justice, U.S. Department of Justice; the National Institute of Standards and Technology, U.S. Department of Commerce; or Aspen Systems Corporation. Points of view or opinions contained within this document are those of the authors and do not necessarily represent the official position or policies of the U.S. Department of Justice.

The National Institute of Justice is a component of the Office of Justice Programs, which also includes the Bureau of Justice Assistance, Bureau of Justice Statistics, Office of Juvenile Justice and Delinquency Prevention, and Office for Victims of Crime.